עבירות מחשב בעשור החולף

מאת

עו"ד נעמי אסיא ועו"ד רחל אלקלעי*

מטרת המאמר של עו"ד נעמי אסיא ועו"ד רחל אלקלעי היא סקירת החקיקה הישראלית בתחום עבריינות מחשבים, תוך התמקדות בעבירת החדירה למחשב, אשר עלתה לכותרות בשנה האחרונה עם חשיפת פרשת "הסוס הטרויאני", וכן בהשוואה לחקיקה האמריקנית בנושא. מטרה נוספת היא להצביע על שינויים הנדרשים, לדעת המחברות, בנוסח החוק.

בתחילת המאמר עוסקות אסיא ואלקלעי במונח "עבירות מחשב" באופן כללי, סוקרות את עבירות המחשב כפי שהן מופיעות בחוק המחשבים, ומתמקדות בעבירה של חדירה למחשב. לקראת סוף המאמר, נערך דיון בסוגיה זו על פי המצב המשפטי בארצות הברית.

לדעת אסיא ואלקלעי, חוק המחשבים אינו מהווה קודיפיקציה של דיני המחשבים, אלא מטפל בעבירות מחשב ובראיות בלבד. לדעתן, נושא עבירות המחשב הינו ייחודי, ועל כן יש לייחד לו חוק מיוחד.

המחברות מגיעות למסקנה, כי ההגדרות הקבועות בחוק המחשבים, שנחקק לפני יותר מעשור, מיושנות ומסורבלות ונקבעו בתקופה בה סביבת העבודה מול המחשב הייתה שונה מזו הקיימת היום. מסקנתן היא, כי יש לתקן את ההגדרות בחוק ולהתאימן לעידן האינטרנט והסלולר של ימינו.

* עו"ד נעמי אסיא – מחברת הספר "דיני מחשבים" ומייסדת משרד עוה"ד נעמי אסיא ושות' המתמחה בדיני מחשבים וקניין רוחני www.computer-law.co.il; עו"ד רחל אלקלעי – דוקטורנטית למשפטים בתחום הקניין הרוחני ועורכת דין בתחום זה במשרד נ' אסיא. המחברות מודות לענבל נבות, מתמחה, על עזרתה.

א. כללי

בימים אלה אנו מציינים עשור לחקיקת חוק המחשבים, התשנ״ה-1995 (להלן: ״**חוק המחשבים**״). המקום המרכזי שהמחשב תופס בחיינו מחד גיסא, והתגברות עבריינות המחשבים מאידך גיסא, גרמו למחוקק הישראלי לבחור בעיצוב חקיקתי לדיני המחשבים הקובע כי מדובר בענף משפטי ממשי ומיוחד, המשותף הן לדין הפלילי והן לדין האזרחי.

> בעולם שבו כל הידע שנצבר, בכל תחום שהוא, כל האינפורמציה, בין אינפורמציה הקשורה לנאס״א ומערכות חלל, ובין אינפורמציה הקשורה לחשבון הבנק או לפרטיו של כל אדם שהוא, מצויה במחשבים, הצורך הראשון במעלה הוא להגן על מאגרי המידע העצומים המצויים במחשבים. אם לא תינתן הגנה שכזו, איש מאיתנו לא יוכל לתפקד, הן בחייו היומיומיים, והן כיחיד מיחידי הציבור, הנזקק והתלוי במאגרי המידע הנוגעים לכלל.[1]

מטרת מאמר זה היא לסקור את החקיקה הישראלית בתחום עבריינות מחשבים, תוך התמקדות בעבירת החדירה למחשב, אשר עלתה לכותרות בשנה האחרונה עם התגלות פרשת ״הסוס הטרויאני״, וכן בהשוואה לחקיקה האמריקנית בנושא. מטרה נוספת היא להצביע על שינויים הנדרשים לדעתנו בנוסח החוק.

ב. עבירות מחשב

המחוקק התייחס בחומרה ובכובד ראש לאפשרויות הרבות שפותחת טכנולוגיית המחשוב בפני העבריינים הפוטנציאליים ולנזקים הכבדים העלולים להיגרם על ידם; סעיפי העבירות מנוסחים באופן כללי ורחב מאוד. לכאורה, יכולות פעולות מחשב רבות ושגרתיות להוות עבירות פליליות, וחלקן אינן דורשות שייגרם כלל נזק.

חוק המחשבים קובע באופן כללי כי כל שינוי, שיבוש, פגיעה בתוכנה או במחשב, חדירה, נטילה וחריגה מהרשאה בשימוש במחשב, הצגת מידע או פלט כוזבים, אשר נעשים שלא כדין, מהווים עבירות פליליות בדרגות חומרה שונות, הגוררות עונשי מאסר שונים של עד חמש שנים.[2]

1 ע״פ (ת״א) 71227/01 **מדינת ישראל נ׳ טננבאום**, תק-מח 2002(2) 1540. פסק הדין ניתן בבית המשפט המחוזי בתל-אביב-יפו ביום 5.6.2002 (להלן: ״**פרשת האנלייזר**״).

2 צוין, כי בהצעות חוק פרטיות שקדמו לחוק המחשבים נקבעו עונשי מאסר של חמש עד חמש-עשרה שנים.

העונשים החמורים הקבועים בחוק, מעידים על חומרת העבירות בעיני המחוקק ועל הרצון להרתיע מפני ביצוען, מתוך הכרה כי רבים מהעבריינים הפוטנציאליים, כגון Hackers צעירים, לא יעשו את המעשים האסורים במידה ויהיו מודעים לחומרת העונשים בגינם. עם זאת, כלליותן של העבירות יכולה כאמור לגרום לכך שהתנהגויות שהיו מקובלות בענף התוכנה טרם חקיקת החוק יוכלו לכאורה להיחשב כעבירות פליליות.[3]

המפתח לפתרון שאלות אלו טמון במשמעות ובפירוש המונח ״שלא כדין״. במקום להתייחס ישירות לדרגת הכוונה הפלילית הנדרשת בעבירות הקיימות בחוק, הוכנס מונח זה בכל עבירות המחשב בחוק, כאחד היסודות הנדרשים לקיומן (למעט בסעיף 3 לחוק המחשבים). משמעותה של הכנסת המושג ״שלא כדין״ היא העברת נטל ההוכחה אל התביעה.

מדיוני ועדת המשנה של ועדת החוקה, חוק ומשפט, שדנה בנוסח החוק עולה, כי הכוונה הייתה לחייב את המשתמש או מבצע הפעולה בקבלת רשות לביצוע הפעולה הספציפית שנחשדת כעבירה, ואם אותה פעולה חרגה מהרשות שניתנה להשתמש במחשב, הרי שהיא תיחשב כאילו נעשתה ״שלא כדין״.

בהסתמך על הפסיקה הקיימת לגבי פירוש מונח זה, נראה, כי הכוונה היא לקיום יסוד של ידיעה לגבי היעדר הרשות לביצוע המעשה (ביצועו שלא ברשות לפי כל דין), ויסוד נפשי של פזיזות לגבי התוצאה העלולה להיגרם בעקבותיו. אין הכוונה כאן לפעולה המתבצעת ברשלנות גרידא.

באמצעות הכנסת יסוד זה, שנטל הוכחת קיומו רובץ על התביעה, ניסה המחוקק למנוע מצב של הרשעה בעבירה פלילית על מעשה שהתבצע ללא רשות ומתוך רשלנות (כגון עובד המבצע במחשב במקום עבודתו פעולה שלא הייתה בגדר סמכותו, וגורם נזק). למעשה, הפסיקה בעשור האחרון דנה בעיקר בתוכנו ובהיקפו המדויקים של יסוד זה.

עבירות המחשב עלולות לפגוע במערכות חיים רבות ולשבשן, והן אף הוגדרו לא אחת כעבירות המתבצעות על ידי אנשים משכילים ואינטליגנטים, שצווארונם נקי ויגיעתם מוחית ולא שרירית.[4]

3 דוגמה אחת להתנהגות כזו היא עובד המשתמש במחשב במקום עבודתו גם לצרכים פרטיים. דוגמה נוספת היא הנוהג של בתי תוכנה לשתול ״פצצות זמן״ (time bombs), בתוכנות מתוצרתם, שהם מנגנונים בתוכנה המפסיקים את פעולתה בתום התקופה בה ניתנה הרשאה להשתמש בתוכנה או המבטיחים את התשלום בעבורה (כגון במקרים של תוכנה שניתנה לניסיון או לתקופת שימוש מוגבלת).

4 ת״פ (ת״א) 5476/03 **מדינת ישראל נ׳ יוסף שי ואח׳**, דינים שלום כו 944. גזר הדין ניתן ביום 2.3.2004.

היטיב להגדיר את אופיין של עבירות המחשב השופט רוזן:[5]

> המדובר בעבירות המתבצעות מחדרים ממוזגים, עבירות המרחיקות לקצווי עולם בזמנים קצרים ונשלטות בידי בודדים המפעילים את כשרונותיהם ומכמני ראשם לפיצוח וחדירה אל תוככי מגירות אישיות, קבצים נסתרים וספריות חשאיות של אנשים פרטיים, חברות ענק ומוסדות ממשלתיים.

גם השופטת ברלינר בפסק הדין בעניין ה״**אנלייזר**״ קבעה, כי: אחד המאפיינים הבולטים של עבירות המחשב הוא היכולת לטשטש בקלות יחסית את העקבות, באופן שהעבריין כמעט אינו חושף עצמו לסכנה, והסיכויים לעלות על עקבותיו שואפים במקרים רבים לאפס.[6]

ג. חוק המחשבים

להלן נסקור את עבירות המחשב, כפי שהן מופיעות בחוק המחשבים, ונתמקד בעבירה של חדירה למחשב.

1. הפרעה לשימוש במחשב או בחומר מחשב

סעיף 2 לחוק המחשבים דן ב״שיבוש או הפרעה למחשב או לחומר מחשב וכן מחיקת חומר מחשב, גרימה לשינוי בו, שיבושו בכל דרך אחרת או הפרעה לשימוש בו הנעשים שלא כדין״.

עבירה זו מבטאת את העיקרון והערך המיוחד של השימוש החופשי במחשב, כחלק ממעמדו המיוחד של המחשב בחיי החברה. מטרתו של סעיף זה הינה להגן על שלמות המידע והתוכנה, ולכן גרימת שינוי או שיבוש חומר מחשב מהווה כעת עבירה שעונשה מאסר שלוש שנים.

יצוין בהקשר זה, כי השימוש במונח ״שלא כדין״ מעביר את נטל ההוכחה אל התביעה, אשר צריכה להוכיח כי: (1) הפעולה נעשתה ללא הסכמתו של בעל המחשב; (2) הפעולה נעשתה ללא היתר שבדין. השימוש במונח נועד להבחין בין פעילות הנופלת במסגרת הסעיף לבין המקרים בהם המעשה בוצע בטעות, בשוגג או בהתרשלות.

5 **שם**.

6 ע״פ (ת״א) 71227/01 **מדינת ישראל נ׳ טננבאום**, תק-מח 2002(2) 1540. ראו לעניין זה גם דבריה של השופטת קמא בת״פ (כפ״ס) 1394/99 **מדינת ישראל נ׳ טננבאום**, בע׳ 6 לגזר הדין.

בת״פ (י-ם) 3813/99 **מדינת ישראל נ׳ רפאלי**,[7] הואשם מר רפאלי, בין היתר, בעבירה על סעיף 2 לחוק המחשבים, לאחר שחדר ממחשב חיצוני למחשב של החברה בה עבד. על מנת למנוע תיעוד כניסתו לרשת בתוכנה לתיעוד פעולות, נהג הנאשם למחוק את התיעוד בכל פעם שהתחבר למחשב.

בית המשפט קבע, לעניין פרשנותו של סעיף 2(2) לחוק המחשבים, כי הפרשנות הנכונה והסבירה של הסעיף היא כי כל מחיקה ו/או שינוי של חומר מחשב הם אסורים לפי החוק. אין כל צורך להוכיח כי המחיקה שבוצעה גרמה לנזק או לשיבוש. עצם המחיקה והשינוי, אסורים.

בעניין זה מעניין לציין, כי בבד״א 144/03 **ועד מחוז ירושלים של לשכת עורכי הדין נ׳ עו״ד מרק צל ואח׳**[8] קבע בית הדין כי מעשיו של הנאשם במחיקת הקבצים אינם הולמים את מקצוע עריכת הדין. כן קבע בית הדין כי לא ימחק עורך דין חומר מחשב, כולל דואר אלקטרוני, מבלי שהוא בעלים מוחלט ובעל שליטה ייחודית בהם, או שהוא מורשה כדין על פי חוזה או אחרת לעשות כן. במקרה זה הגיע בית הדין למסקנה כי יש לייחס חומרה רבה למחיקת הקבצים ע״י הנאשם, לאור העובדה כי לא הייתה מניעה להגיע להסכמה עם השותפים בדבר העתקת או מחיקת הקבצים.

2. עבירות מרמה באמצעות מחשב

סעיף 3 לחוק המחשבים עוסק בלב ליבן של העבירות המתבצעות באמצעות מחשב – שינויים במידע שתכליתם לקבל דבר במרמה. הסעיף קובע עונש מאסר של חמש שנים למי ש״מעביר לאחר או מאחסן במחשב מידע כוזב או עושה פעולה לגבי מידע כדי שתוצאתה תהיה מידע כוזב או פלט כוזב, או כותב תוכנה, מעביר תוכנה לאחר או מאחסן תוכנה במחשב, כדי שתוצאת השימוש בה תהיה מידע כוזב או פלט כוזב, או מפעיל מחשב תוך כדי שימוש בתוכנה כאמור״.

קיומה של עבירה זו נועד להתמודד עם בעיות של זיוף, מרמה וגניבה, וכן מבטא את מגמת ההרתעה של החוק בקביעת רמת ענישה של חמש שנות מאסר בגין עבירה זו.

3. חדירה שלא כדין לחומר מחשב

אחת העבירות היסודיות והמרכזיות שבחוק המחשבים הינה עבירת החדירה לחומר מחשב שלא כדין, הקבועה בסעיף 4 לחוק. הסעיף קובע מאסר של שלוש שנים למי ש״חודר שלא כדין לחומר מחשב הנמצא במחשב״. חדירה לחומר מחשב מוגדרת כ-

7 דינים-שלום טז 861.

8 בד״א 144/03 **ועד מחוז ירושלים של לשכת עורכי הדין נ׳ עו״ד מרק צל ואח׳**. פסק הדין ניתן בבית הדין המשמעתי הארצי של לשכת עורכי הדין ביום 15.6.2004.

״חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, התשל״ט-1979״.

החדירה למחשב הוגדרה במדינות רבות בעולם כעבירה פלילית, בעיקר בשל העובדה כי החדירה למחשב מהווה שלב הכרחי בדרך לביצוע עבירות נוספות באמצעות המחשב. מדובר בחדירה אקטיבית, להבדיל מחדירה לחומר מחשב שהיא האזנה לפי חוק האזנות סתר.[9]

הבעייתיות בהגדרת המונח ״חדירה״ הועלתה בהרחבה בת״פ (י-ם) 3047/03 **מדינת ישראל נ׳ מזרחי**,[10] שם ציין השופט טננבוים, כי על אף שהסעיף אכן מגדיר חדירה לחומר מחשב, הרי שאין הגדרה מספקת לחדירה למחשב ואין כל ביאור בהיר למונח ״חדירה״. גם פרופ׳ קר טען במאמרו[11] כי עד היום אין תפישה ברורה לשאלה מהי אותה חדירה שלא כדין ומהם מאפייניה הבולטים. לדעת פרופ׳ קר, במצב הקיים של תקשורת בין מחשבים, הרי שהחדירה קיימת כמעט תמיד, ואת ההבדל בין חדירה מותרת לאסורה יש למצוא ביסוד של ״שלא כדין״.[12]

בפסק הדין בעניין **מזרחי** זוכה הנאשם, לאחר שחדר לאתר האינטרנט של המוסד, בשל העובדה כי בית המשפט השתכנע שהנאשם ביקש אך ורק לבדוק את אבטחת האתר. השופט טננבוים דן בהכרעת הדין בנושא פרשנות המונח ״שלא כדין״. בעניין זה נקבע, כי לפי הפרשנות של הסעיף הישראלי, הרי שהחדירה למחשב היא עצמה אסורה.[13] אולם, השאלה שעמדה במסגרת פסק הדין הינה אם בדיקת אבטחתו של אתר מותרת, אם לא. התשובה לשאלה זו אינה חד משמעית, ובית המשפט קבע כי לא ניתן לקבוע באופן מוחלט מהו הסיווג המשפטי של בדיקת אבטחה.

9 להרחבה ראו: R. W. Downing "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" 43 **Colum. J. Transat's L.** (2005) 705. במאמר זה גם דיון נרחב בשאלה מה בין חדירה למחשב על ידי צד בלתי מורשה לבין חדירה למחשב על ידי גורם מורשה אך שחרג מגבולות סמכותו. כותב המאמר ממליץ לכל המדינות החתומות על האמנה, כמו גם מדינות נוספות, לאסור את שני סוגי החדירה למחשב בחקיקתן המדינתית.

10 ת״פ (י-ם) 3047/03 **מדינת ישראל נ׳ מזרחי**, דינים-שלום כו 426. ניתן בבית משפט השלום בירושלים מפי השופט טננבוים ביום 29.2.2004.

11 O. S. Kerr "Cybercrime's Scope: Interpreting "Access" and "Autorization" in Computer Misuse Statuter" Vol. 78 No. 5 **New York University Law Review** (November 2003) pp. 1596-1668.

12 דעה זו של פרופ׳ קר טרם אומצה במשפט הישראלי, אולם היא מהווה הוכחה נוספת לבעייתיות המושג ״חדירה״. ראו לעניין זה דבריו של השופט טננבוים בהערה 10 **לעיל**.

13 זאת, בדומה לדין האירופי, שלפיו עצם החדירה למחשב אסור בלא קשר לגרימת נזק, ובניגוד לגישה האמריקנית, לפיה החדירה אסורה אך ורק אם היא מלווה בשימוש לא-מורשה או בגרימת נזק למחשב.

הקביעה, כי מדובר בשימוש מותר או אסור, תלויה בנסיבות שבהן נעשתה הבדיקה. אם הבדיקה מהווה מעשה עצמאי לחלוטין שלא נועד לפגוע, הרי מדובר בבדיקה כשרה. אולם, אם מדובר בבדיקה שמהווה שלב מקדים לניצול חורי אבטחה ולחדירה למחשבים שונים, הרי שבדיקה זו מהווה ניסיון לעבירה.

בסיפא של פסק הדין, מעיר השופט טננבום הערה לעניין פרשנותו של חוק המחשבים באורח התואם את רוח האינטרנט ומבנהו. עמדתו העקרונית היא, כי יש להיזהר בהיקשים מחוקים פליליים רגילים לחוקים הנוגעים לעולם האינטרנט, משום שהחוקים הפליליים הרגילים מתייחסים לעולם המבוסס על קניין פרטי ברור ומוגדר, בעוד שהאינטרנט מבוסס על שיתופיות ועל משאבים העומדים לשירות הכלל. עוד מציין השופט טננבום, כי כאשר מדובר בחקיקת אינטרנט, יש לפרשה באופן שיעזור לעולם האינטרנט להמשיך להתפתח קדימה ולטובת הציבור, ולא בצורה שתגביל, תפריע ותעכב התקדמות זאת.

מכאן עולה המסקנה, כי בדיקתה של אבטחת אתרים הינה פעילות חיובית בעיקרה, שעקרונית יש לעודדה ולהיזהר מלפגוע בה.

פסק דין חשוב בעניין חדירה למחשב הוא פסק הדין בעניין ה״**אנלייזר**״.[14] הנאשם, אהוד בן צבי טננבאום, חדר שלא כדין באמצעות האינטרנט לעשרות רבות של מחשבים בארץ ובחו״ל. בין היתר חדר הנאשם למערכת מחשבי נאס״א, למחשבים של מוסדות ממשל וצבא בארה״ב וכן למחשבי אתר הכנסת ואתר הנשיא.

בפסק הדין בערכאת הערעור נקבע, כי פעילותו של הנאשם לא הסתכמה בחדירה בלבד, אלא התבטאה גם במה שכינתה ע״י התביעה כ״וונדליזם אלקטרוני״.[15] גם בפסק דין זה השווה בית המשפט את עבירת החדירה למחשב לעבירת הפריצה, וקבע, כי חדירה למחשב היא פריצה לכל דבר ועניין, ואין הבדל בין מי שמטפס כדי לפרוץ לבניין לבין מי שמוצא את הדרך לפרוץ למחשב. בסופו של עניין גזר בית המשפט על אהוד טננבאום מאסר בפועל של שנה וחצי.

מפסקי דין נוספים העוסקים בסוגיית החדירה לחומר מחשב עולה כי החדירה לחומר מחשב מלמדת על מידה רבה של מסוכנות, והיא מהווה עבירה התנהגותית ללא כל רלוונטיות לתוצאת החדירה.[16] לעניין חזקת המסוכנות בעבירות החדירה לחומר מחשב, נקבע בפסק הדין בעניין **מונדיר,** כי ״הסיכונים לחברה וליחידיה הם מסוגים שונים ומגוונים, ובחברה בת זמננו בה לאמצעי התקשורת ולמחשוב יש תפקיד כה

14 ראו **לעיל** הערה 6.

15 **שם**. ראו לעניין זה דבריה של השופטת ברלינר ״כאשר מדובר בהשתלת וירוס ועריכת שינויים וכיוצא בכך, שמחייבים לאחר מכן פעילות מתמשכת תוך השבתת האתרים כדי לשקם את ההרס שזרע המשיב, הרי אין הגדרה הולמת יותר מאשר ׳וונדליזם אלקטרוני׳ ״.

16 ראו ת״פ (ת״א) 40250/99 **מדינת ישראל נ׳ מונדיר בדיר ואח׳**. בהחלטה מיום 8.8.99 נקבע, כי ״החדירה למערכות מחשב באמצעים מתוחכמים.. השיטתיות של ביצוע העבירות, החזרה וההתמדה בביצוע אף היא מלמדת על מידה רבה של מסוכנות...״.

מרכזי, פעולות שיטתיות מהסוג המיוחד לעוררים הן פעולות שיש בהן, בנסיבות מסוימות, כדי לסכן את ביטחון הציבור ואת סדרי החברה התקינים״.[17]

לאחרונה, בסוג אחר של חדירה שלא כדין למחשב, הוגש כתב אישום נגד עורך דין מיוקנעם אשר ביקש לנקום בצעירה שביקשה לסיים את מערכת היחסים שלה איתו. עורך הדין עשה זאת, לכאורה, בדרך מקורית במיוחד. על פי כתב האישום, הוא הצליח לחדור לתא הדואר האלקטרוני של הצעירה לאחר שהשיג את סיסמת הכניסה לתא הדואר האלקטרוני שלה, הוא נכנס לתיבה ללא ידיעתה ב-50 הזדמנויות שונות, וקרא את המכתבים שנשלחו אליה. לאחר שעיין במספר הודעות דוא״ל שאותן קיבלה משני גברים שונים, פנה לנשותיהם והודיע להן כי הם מנהלים רומן עם הצעירה.[18] מעניין יהיה לעקוב אחר פסיקת בית המשפט בפרשה שהחלה באפריל 2005 וטרם ניתן בה פסק דין.

חדירה למחשב באמצעות ״הסוס הטרויאני״

בשנה האחרונה עלתה לכותרות בישראל פרשת ״הסוס הטרויאני״. הפרשה התחילה כאשר הסופר אמנון ז׳קונט הגיש תלונה במשטרה, שלפיה חלקים מספרו החדש מופצים באינטרנט לפני שהסתיימה כתיבתו. לאחר סריקת מחשבו של ז׳קונט התגלה בו ״סוס טרויאני״ שבאמצעותו נשלחו מסמכים ותמונות לשרת FTP. בהמשך השנה נחשפו בישראל פרשות ריגול במחשבי החברות הגדולות במשק והוגשו כתבי אישום. הפרשות הנ״ל מדגישות את החשיבות הרבה שיש להגנה על מאגרי מידע ועל רמת התחכום של העבריינים.

מהו ״סוס טרויאני״? בשונה מווירוס מחשב או מתולעת מחשב,[19] ״סוס טרויאני״ הינו תוכנת מחשב המכילה קוד מחשב מזיק, אשר עם קבלת שליטה במחשב מסוגל לבצע נזק רב, כגון מחיקת קבצי מחשב. התוכנה חודרת למחשב, בדרך כלל, דרך רשת האינטרנט תוך התחזות לתוכנה תמימה. ישנם סוסים טרויאניים שתפקידם לתת הרשאות למשתמש אחר להיכנס מרחוק למחשב הנפגע. פעולה זו נקראת גם התקנת ״דלת אחורית״ (backdoor). סוסים טרויאניים אחרים הם ״רוגלה״, כלומר איסוף מידע (למשל מספרי כרטיסי אשראי שהמשתמש מקליד) מהמחשב שבו הותקנו ושליחתו ליעד מוגדר מראש.

17 **שם**. בהחלטה מיום 7.9.99.

18 במקרה זה טען ב״כ הנאשם, כי אין כאן עבירה על חוק המחשבים, וזאת, בין היתר, מפני שהאינפורמציה אשר נטען כי נקראה אינה נופלת בגדר ההגדרה של ״חומר מחשב״ על פי החוק. ראו: http://www.ynet.co.il/articles/0,7340,L-3098814,00.html.

19 וירוס מחשב הוא תוכנה אשר מעתיקה את עצמה לתוכנה אחרת ונעשית פעילה כאשר התוכנה מורצת. תולעת מחשב משכפלת את עצמה וגורמת לפגיעה במשאבי המחשב.

מלבד עבירה על פי חוק המחשבים, התקנת ״סוס טרויאני״ מהווה לכאורה שורה של עבירות אחרות כהאזנת סתר אסורה, וכן ניתן לטעון לפגיעה בפרטיות על פי חוק הגנת הפרטיות האוסר על התחקות אחר אדם שעלולה להטרידו. עוולה אפשרית נוספת היא גזל של סוד מסחרי, שהוא עוולה על פי חוק עוולות מסחריות.

4. חדירה לחומר מחשב כדי לעבור עבירה אחרת

סעיף 5 לחוק המחשבים קובע, כי מי שעושה מעשה אסור לפי סעיף 4 לחוק זה, כדי לעבור עבירה אחרת, דינו מאסר חמש שנים. הסעיף נועד להדגיש את החומרה שבה רואה המחוקק שימוש לרעה ביכולות המתקדמות של טכנולוגיית המחשוב לצרכים פליליים, וכן להרתיע מפני שימוש במחשב ככלי לביצוע עבירות פליליות אחרות. העונש שמוטל על העובר עבירה לפי סעיף זה הינו חמור, ללא קשר לחומרת העבירה שאותה תכנן העבריין לבצע (אף אם אותה עבירה הייתה מסוג חטא או עוון).

5. נגיף מחשב

סעיף 6 לחוק המחשבים קובע כי:

> (א) העורך תוכנה באופן שהוא מסגלה לגרום נזק או שיבוש למחשב או לחומר מחשב בלתי מסויימים, כדי לגרום שלא כדין נזק או שיבוש למחשב או לחומר מחשב, מסויימים או בלתי מסויימים, דינו – מאסר שלוש שנים.
>
> (ב) המעביר לאחר או המחדיר למחשב של אחר תוכנה אשר סוגלה לגרום נזק או שיבוש כאמור בסעיף קטן (א), כדי לגרום שלא כדין נזק או שיבוש כאמור, דינו – מאסר חמש שנים.

סעיף זה חוקק עקב הנזק המיוחד ורחב ההיקף של תופעת נגיפי המחשב, כאשר העבירה או ההחדרה של הוירוס למחשב הופכת את העבירה לחמורה יותר.

בת״פ (ת״א) 2591/04 **מדינת ישראל נ׳ אנור בני**[20] הואשם הנאשם, בין היתר, בעריכת נגיף מחשב ובהעברת נגיף מחשב לאחר שערך תוכנה שבעזרתה ניתן לחשוף בפני שולח התוכנה את שם המשתמש וסיסמתו של המשתמש. ובמילים אחרות, הנאשם יצר וירוס מחשב המאפשר לו לפלוש למחשביהם של אחרים ולעשות שימוש שלא כדין בכל שאצור בהם. נוסף לכך, פנה הנאשם לאחת העובדות בחברת תוכנה מסוימת והציע לה לרכוש את התוכנה שערך בשפת מקור. בית המשפט קבע, כי מדובר ״בעבירות שהן פרי תכנון קר וציני ולצורך הפקת רווחים גדולים שלא כדין ועל חשבון הזולת״. אשר

20 ת״פ (ת״א) 2591/04 **מדינת ישראל נ׳ אנור בני**. ניתן ביום 31.10.2004 בבית משפט השלום בתל אביב על ידי השופט חנן אפרתי.

על כן, גזר בית המשפט על הנאשם 24 חודשי מאסר, מתוכם שישה חודשי מאסר בפועל שירוצו בעבודות שירות, וכן קנס כספי.

בת״פ (ת״א) 5467/03 **מדינת ישראל נ׳ יוסף שי ואח׳**[21] הודה הנאשם בעבירות מחשב, וביניהן הפצת וירוס וחדירה למחשבים. השופט דוד רוזן מבית משפט השלום בתל אביב פסק, כי ״עבירות המחשב הן עבירות נואלות וקשות. חומרתן אינה פחותה מעבירות פליליות אחרות. השימוש ההולך ומתרבה במחשבים, ועוצמת ההיזקקות להם מחייבים את ביהמ״ש ליתן שיניים לחוק המחשבים. שומה על ביהמ״ש להשית עונשים שיהא בהם כדי להרתיע עבריינים בכוח״. בסופו של דבר, גזר בית המשפט על הנאשם שישה חודשי מאסר על תנאי למשך שלוש שנים.[22]

בוועדת המשנה להצעת חוק המחשבים נדונה השאלה אם יש להוסיף לחוק גם את העבירה ״המחזיק תוכנה שלא כדין לשם שימוש בעל אופי מסחרי או לשם הגשת יתרון מסחרי דינו מאסר 3 שנים״.[23] גם בתזכיר החוק משנת 1987[24] הוצע לקבוע עבירת ״השגת תוכנה שלא כדין״, שהעונש עליה יהא חמש שנות מאסר.

החלטת הוועדה, בסופו של דבר, הייתה להשאיר נושא זה לחקיקת זכויות יוצרים.[25] מאז עבר עשור שלם וחוק זכויות יוצרים חדש עדיין אין. לעומת זאת, הועלו הצעות כי בעוד שיישום החוק ואכיפתו לגבי עבירות מחשבים יהא כנראה מצומצם (כפי שאכן קרה בפועל), הרי שלגבי עבירות של שימוש מסחרי בלתי חוקי בתוכנה, יהא היישום רחב ומיידי. מכל מקום, הוחלט כאמור לא להרחיב את החוק בנושא זה.

ד. פרשנות המונח ״שלא כדין״

המפתח לפרשנות העבירות לפי חוק המחשבים, כפי שצוין לעיל, הינו באמצעות מתן פירוש למונח ״שלא כדין״. במקום להתייחס ישירות לדרגת הכוונה הפלילית הנדרשת

21 ת״פ (ת״א) 5476/03 **מדינת ישראל נ׳ יוסף שי ואח׳**, דינים שלום כו 944, ניתן ביום 2.3.2004 בבית משפט השלום בתל אביב ע״י השופט דוד רוזן.

22 יצוין, כי בפסק הדין הראשון בנושא נגיף מחשב – ת״פ (חי׳) 8243/97 **מדינת ישראל נ׳ גיל פז**, דינים-שלום יב 153, נידון הנאשם ל-6 חודשי עבודות שירות ול-12 חודשי מאסר על תנאי.

23 ראו לעניין זה דבריה של כותבת מאמר זה בפרוטוקול מס׳ 1 מישיבת ועדת המשנה להצעת חוק המחשבים (של ועדת החוקה, חוק ומשפט) מיום 24.1.1995 בע׳ 12: ״אנו הצענו לומר: ׳המחזיק תוכנה שלא כדין לשם שימוש בעל אופי מסחרי או לשם השגת יתרון מסחרי – דינו מאסר 3 שנים׳. המקבילה לסעיף הזה קיימת בחוק זכויות יוצרים האמריקאי והאיטלקי״.

24 תזכיר חוק המחשבים (עבירות, הגנת תוכנה וראיות), התשמ״ז-1987 (להלן: ״**תזכיר שלגי**״).

25 **שם**. ראו לעניין זה דבריו של מיגל דויטש: ״יכול להיות מאד, שיש מקום לתיקון בתוך חוק זכויות יוצרים בתוך הפקידה... ישנן כל מיני הגנות בדיני זכויות יוצרים, שהנתבע זכאי להן. אנו לא נוכל להתנתק, לשלוף את זה משם ולהעביר את זה לתוך קרקע שבכלל לא מתאימה״.

בעבירות הקיימות בחוק, נכלל מונח זה בכל עבירות המחשב בחוק כאחד היסודות הנדרשים לקיומן (למעט בסעיף 3 לחוק המחשבים).

בהסתמך על הפסיקה הקיימת לגבי פירוש מונח זה, נראה, כי הכוונה היא לקיום יסוד של ידיעה לגבי העדר הרשות לביצוע המעשה (ביצועו שלא ברשות לפי כל דין), ויסוד נפשי של פזיזות לגבי התוצאה העלולה להיגרם בעקבותיו. אין הכוונה כאן לפעולה המתבצעת מתוך רשלנות גרידא.

במסגרת דיוני ועדת המשנה של ועדת החוקה, חוק ומשפט שדנה בנוסח החוק, עלה, כי הכוונה הייתה לחייב את המשתמש/מבצע הפעולה בקבלת רשות לביצוע הפעולה הספציפית שנחשדת כעבירה; אם אותה פעולה חרגה מהרשות שניתנה להשתמש במחשב, הרי שהיא תיחשב כאילו נעשתה ״שלא כדין״. כלומר, המונח ״שלא כדין״ הוכנס כדי למנוע, בין היתר, פעולות שנעשו שלא מתוך מחשבה וכוונה פלילית.[26]

נראה, כי באמצעות הכנסת יסוד זה, שנטל הוכחת קיומו רובץ על התביעה, ניסה המחוקק למנוע מצב של הרשעה בעבירה פלילית על מעשה שהתבצע מתוך רשלנות (כגון עובד המבצע במחשב במקום עבודתו פעולה, שלא הייתה בגדר סמכותו, וגורם נזק).

כך, למשל, הציעה כותבת מאמר זה בישיבת ועדת המשנה להצעת חוק המחשבים,[27] שבכל מקום בו כתוב ״שלא כדין״ יש לכתוב אף ״בזדון״. זאת, לנוכח העובדה כי במסגרת עבודת התכנות עצמה ישנן פעולות רבות שנעשות, כמו למשל ״באגים״, וניתן בהחלט לצפות שמישהו ירצה ״להתלבש״ על תוכניתן שעשה ״באגים״ בשוגג.

ה. ענישה

כפי שצוין לעיל, התייחס בית המשפט במקרים רבים לחומרת הענישה שיש להשית על מנת להרתיע עברייני מחשב.

26 לעניין זה ראו דבריה של עו״ד נעמי אסיא בפרוטוקול מס׳ 3 מישיבת ועדת המשנה להצעת חוק המחשבים (של ועדת החוקה, חוק ומשפט) מיום 14.2.1995, בע׳ 19: ״מאוד מסוכן להיכנס למצב נפשי של התרשלות״.
כן ראו דבריו של מ׳ דויטש בע׳ 18 לפרוטוקול: ״ההצעה האופרטיבית שלי לפחות היא להוסיף בסעיף 8(א), בעקבות ההערות: ׳כדי לגרום שלא כדין נזק או שיבוש׳״. לדעתו, ואנו מסכימים, כי המונח ״שלא כדין״ פתר את נושא הכוונה הפלילית.

27 ראו פרוטוקול מס׳ 3 מישיבת ועדת המשנה להצעת חוק המחשבים (של ועדת החוקה, חוק ומשפט) מיום 14.2.1995, בע׳ 15.

השופטים בערכאת הערעור בפסק הדין בעניין ה״**אנלייזר**״[28] לא יכלו לקבל את הפער הגדול בין הכרעת הדין של שופטת בית משפט השלום בכפר סבא, שם היא מציגה במלוא החומרה את פעולותיו של ״**האנלייזר**״, אל מול גזר הדין הרחום שאינו שולח אותו לרצות מאסר של ממש. על כן, שלחו השופטים ברלינר, המר וכספי את אהוד טננבאום לרצות שנה וחצי של מאסר בפועל.

השופטת ברלינר היטיבה לציין לעניין הצורך בקביעת נורמת ענישה ראויה, כי:

> בעולם שבו כל הידע שנצבר, בכל תחום שהוא... מצוי במחשבים, הצורך הראשון במעלה הוא להגן על מאגרי המידע העצומים המצויים במחשבים. אם לא תינתן הגנה שכזו, איש מאתנו לא יוכל לתפקד.

השופט המר הצטרף לדעת חברתו וטען כי האינטנסיביות, הנועזות, חוסר המעצורים וריבוי העבירות חובקות העולם על פני תקופה ארוכה, הנזקים הישירים והעקיפים, האינטרס הציבורי והחשיבות ההולכת וגוברת בעולם המודרני של מחשב ומאגרי מידע – כל אלה מחייבים הצבת רף ענישה חמור יותר.

בעניין זה ציין גם השופט רוזן,[29] כי השימוש ההולך ומתרבה במחשבים ועוצמת ההיזקקות להם, מחייבים את בית המשפט ליתן שיניים לחוק המחשבים. שומה על בית המשפט להשית עונשים שיהא בהם כדי להרתיע עבריינים בכוח.

העונשים החמורים הקבועים בחוק מעידים על חומרת העבירות בעיני המחוקק, ועל הרצון להרתיע מפני ביצוען, מתוך הכרה כי רבים מהעבריינים הפוטנציאלים, כגון Hackers צעירים, לא יעשו את המעשים האסורים אם יהיו מודעים לחומרת העונשים בגינם. עם זאת, כלליותן של העבירות עשויה כאמור לגרום לכך שהתנהגויות שהיו מקובלות בענף התוכנה טרם חקיקת החוק יוכלו לכאורה להיחשב כעבירות פליליות.[30]

כדברי השופטת ברלינר:

> הצורך הוא לשדר מסר ברור כלפי אותו פלח ציבור שממנו יכולים לבוא העבריינים הפוטנציאלים, קרי אנשים צעירים, נורמטיביים, שרקע חייהם תקין, ובמרבית המקרים כישוריהם השכליים למעלה מן הממוצע. נגד עיניהם של אלה צריכה להידלק נורה אדומה בכל פעם שהפיתוי הקל והזמין לפרוץ למחשב יעבור במוחם.[31]

28 **לעיל** הערה 6.

29 **לעיל** הערה 6.

30 דוגמה להתנהגות כזו היא עובד המשתמש במחשב במקום עבודתו גם לצרכים פרטיים.

31 **לעיל** הערה 6.

ו. ארצות הברית

משרד המשפטים האמריקני חילק לשישה סוגים את העבירות המתאפשרות באמצעות מחשב או אינטרנט:[32]

א. שימוש במחשב כדי לבצע פשע.
ב. הימורים באינטרנט.
ג. הטרדה באמצעות האינטרנט.
ד. פעילות בלתי חוקית באינטרנט.
ה. פורנוגרפיה הקשורה לילדים.
ו. מכירה של תרופות הדורשות מרשם (ללא מרשם) באינטרנט.

לסיווג זה ניתן להוסיף גם:

א. גישה בלתי מורשית לרשתות מחשב.
ב. יצירה והפצה של וירוסים.
ג. הפרעה למתן שירות.
ד. מכירה בלתי מורשית של חומר המוגן בזכויות יוצרים.

בשל קוצר היריעה נתמקד במאמר זה בעבירת החדירה למחשב בלבד.

1. עבירת החדירה למחשב בארה״ב – חקיקה פדרלית ומדינתית

בארה״ב ניתן לתבוע עברינים החודרים למחשב של אחר על פי חוק ה-**Computer Fraud and Abuse Act 1986 (US) 18 U.S.C 1030**. חוק זה מנוסח מתוך תפישה עתידית רחבה, במטרה לאפשר התאמה לשינויי הטכנולוגיה התכופים.[33]

סעיף 1030 (a) מפרט שבעה סוגים שונים של עבירות מחשב.

ס״ק (1) מגן על חיסיון של מידע מסווג. הסעיף קובע, כי כדי לבצע עבירה על פי ס״ק זה, על העבריין לבצע גישה שלא בסמכות ולהשיג מידע מסווג, אשר הוגדר על ידי הממשל כמסווג.

ס״ק (2) מגן על חיסיון של מידע שאינו מסווג. הסעיף אוסר על השגת מידע הנוגע למוסד פיננסי או לחברת אשראי, מידע הנתון לחזקתו של הממשל או כל מידע פרטי הקשור בין מדינות למסחר חוץ.

32 See United States Dep't of Justice, Computer Crime and Intellectual Property Section (CCIPS), available at http://www.cybercrime.gov/crimes.html.

33 E. J. Sinrod & W. P. Reilly "Cyber-Crimes: A practical Approach to the Application of Federal Computer Crime Laws" 16 **Santa Clara Computer & High tech L.J.** 177.

ס״ק (3) בא למנוע הסגת גבול נגד מחשבי הממשל.
ס״ק (4) בא להגן מפגיעה ברכוש תוך שימוש במחשב וקובע כי מי שתוך מעשהו זה משיג כל דבר בעל ערך מבצע את העבירה. למרות זאת, אם הדבר שהושג הינו בעל ערך נמוך מחמשת אלפים דולר – יש בכך חריג לתחולת הסעיף.

ס״ק (5) קובע שלוש עבירות:

א. מי שגרם להעברתם של תוכנה, מידע קוד או פקודה ועקב כך גרם בכוונה לנזק למחשב מוגן מבצע פשע. אין זה משנה אם אותו עבריין הינו האקר חיצוני או עובד פנימי של הניזוק. נזק מוגדר כפגיעה בשלמות או זמינות הנתונים, תוכנית או מערכת או אינפורמציה אשר גורמת לאובדן בשווי של לפחות 5000 דולר במשך שנה לפחות. תביעה שלא מגיעה לסכום נזק של 5000 דולר יכולה להיות מוגשת בבתי משפט לא פדרליים בעוולה של הסגת גבול במיטלטלין.
ב. אדם אשר בכוונה מבטיח גישה למחשב מוגן שלא בסמכות וכתוצאה מכך גורם נזק בפזיזות, יואשם בביצוע פשע.
ג. אדם אשר בכוונה מבטיח גישה למחשב מוגן שלא בסמכות, וכתוצאה מכך גורם לנזק, יואשם בעוון.

ס״ק (6) אוסר מסחר בקודי גישה או בכל מידע אשר בעזרתו ניתן להבטיח גישה לא מורשית למחשב, אם סחר זה משפיע בין מדינות או כאשר המחשב אליו רוצים להבטיח גישה שלא בסמכות נעשה בו שימוש עבור הממשל או על ידי הממשל.
ס״ק (7) מעניש האקר אשר בכוונתו לסחוט כסף או כל דבר בעל ערך מכל אדם, חברה, מוסד חינוכי, מוסד פיננסי, ארגון או גוף ממשלתי אחר, מאיים לגרום נזק למחשב מוגן.[34]

יצוין, כי להבדיל מהחוק הישראלי בולטת בחוק זה ההגנה הרחבה הניתנת לאינטרסים הנוגעים לממשל.

כמו כן ישנה אפשרות להגיש תביעה לפי חוקים נוספים של האזנת סתר (Wiretap Act)[35] אשר קובע עבירה פלילית ואחריות אזרחית למי אשר:

> …intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercep.[36]

34 להשוואה בין היסוד הנפשי בעבירות המחשב במשפט הישראלי לבין המשפט האמריקני ראו: א׳ קוסטיקה ״היסוד הנפשי בעבירות מחשב״ אתר פסק דין (www.psakdin.co.il).

35 See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 801-804, 82 Stat. 197, 211-23 (codified as amended at 18 U.S.C. 2510-2522 (2000 & Supp. II 2002)).

36 See 18 U.S.C. 2511(1)(a) (2000).

האזנה לתקשורת מוגדרת בחוק זה כשימוש בכל מכשיר אלקטרוני או מכני כדי להשיג את תוכנו, לרבות תקשורת אלחוטית כבלים וכיו״ב.[37]

חוק נוסף הוא ה-**Stored Communications Act (SCA):**[38] החוק דורש להראות שנתבע השיג, שינה או מנע גישה מורשית לתקשורת ״בעת איחסון אלקטרוני״ במתקן אשר דרכו מסופקת תקשורת אלקטרונית.

כמו כן, חוק ה-Electronic Communications Privacy Act משנת 1986, מכוון לעבירות של שינוי או מניעת גישה מורשית למקום אחסון אלקטרוני.

נוסף על חקיקה זו קיימת חקיקה מדינתית חדשה ויוזמות חקיקה במספר רב של מדינות בארה״ב בנושא זה:[39]

למשל, בקליפורניה נחקק בשנת 2004 חוק המכיל איסורים רבים בנושא עבירות החדירה למחשב, לרבות איסור על החדרת תוכנה המעתיקה את עצמה למחשב אחר, איסור על עריכת שינוי בהגדרות המתייחסות לאופן הגישה למחשב, איסור על איסוף מידע באמצעי מרמה ואיסור על מניעה ללא רשות של מאמצי המשתמש למנוע התקנה של תוכנת רוגלה.

2. פסיקה בארה״ב לעניין עבירת החדירה למחשב

התביעה בארה״ב, בעניין עבירות חדירה למחשב, עניפה ביותר. לשם דוגמה: באוגוסט 2005 הורשע בארה״ב יצרן ומשווק של ״סוס טרויאני״ המכונה LoverSpy. הנתבע, אנריקה פרז, יצר ומכר את תוכנת ״הסוס הטרויאני״ כשהיא מוסווית בתוך כרטיסי ברכה אשר נשלחו באמצעות דואר אלקטרוני. מרגע שהנמען פתח את הדואר האלקטרוני שלו, עקב ״הסוס הטרויאני״ אחר מידע ואסף את כל המידע אשר הוקלד על ידי המשתמש, ושלח אותו למבקש ישירות או דרך המחשב של הנתבע. ״הסוס הטרויאני״ גם איפשר למבקש לשלוט במחשב של הקרבן. הנתבע הואשם על פי מספר עבירות וביניהן ה-CFAA, בעבירה של חדירה בלתי מורשית למחשבים מוגנים על מנת להשיג רווח פיננסי.[40] כן הורשע בעבירה של האזנת סתר.[41]

37 18 U.S.C. 2510(12).

38 See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 201202, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. 2701-2709, 2711-2712 (2000 & Supp. II 2002).

39 לסקירה על יוזמות חקיקה בתחום זה בארה״ב ראו: http://www.ncsl.org/programs/lis/spyware04.htm. כן ראו סקירה נרחבת של החקיקה הפדרלית והמדינתית בארה״ב במאמר: H. Jacobson & R. Green "Computer Crime" 39 **Am. Crim. L. Rev.** (2002) 273.

40 Title 18, United States Code, Sections 1030(a)(2)(c) and (c)(2)(b)(I).

41 למידע נוסף ראו: www.usdoj.gov/criminal /cybercirme/perezindict.htm.

לאחרונה התחוללה ברחבי העולם סערה של ממש בעקבות פרשת ״הסוס הטרויאני״ של חברת BMG SONY.

במטרה למנוע צריבת דיסקים והמרת קבצי מוזיקה, שילבה חברת הענק בדיסקים שלה מעין ״סוס טרויאני״ (תוכנת rootkit), שגרם למחשבי הגולשים נזק גדול ופער חור אבטחה במחשבי המשתמשים. ״עדכון תוכנה״ ששחררה סוני בהבטחה שיסיר את ה-rootkit, לא רק שלא הסיר את הקוד, אלא אף לווה בהודעת שחרור אשר התעלמה מסכנות האבטחה שהחדרת קוד מסוג זה גרמה. רישיון השימוש המלווה את תקליטורי המוסיקה של סוני התיר לחברה, בין השאר, לשתול במחשב המשתמש ״דלת אחורית״ שתאפשר לה לעקוב אחרי השימוש בקבצי המוסיקה. חקירת אבטחה העלתה שמעל 500,000 רשתות מחשבים, כולל רשתות ממשל ורשתות צבאיות, נדבקו ב-rootkit של סוני.

בעקבות פרשה זו הוגשה על ידי ״החזית האלקטרונית״ (EFF), ארגון אמריקני שלא למטרות רווח העוסק בהגנה על זכויות בסביבה המתוקשבת, תביעה ייצוגית נגד סוני BMG. נוסף לכך הוגשה תביעת פיצויים נגד סוני על ידי מדינת טקסס על פי חוק ה-Texas Consumer Protection Against Computer Spyware Act of 2005, אשר מגן על צרכנים מפני תוכנות רוגלה נסתרות. התביעה ביקשה פיצויים בסך 100,000 דולר בגין כל הפרה של החוק.

ז. סוף דבר

חוק המחשבים אינו מהווה קודיפיקציה של דיני המחשבים, אלא מטפל בעבירות מחשב ובראיות בלבד, בהתאם לתזכיר חוק המחשבים (עבירות, הגנת תוכנה וראיות), התשמ״ז-1987.

הצעת חוק המחשבים[42] ביקשה לקבוע הוראות עונשיות מיוחדות להגנה על אינטרסים מופשטים, כגון חומר מחשב, וזאת – גם אם קיימים איסורים אשר ניתן למצוא להם אחיזה בהוראות דיני העונשין הקיימות. לדעתנו, נושא עבירות המחשב הינו ייחודי, כך שיש לייחד לו חוק מיוחד.[43]

מלבד ההוראות העונשיות, קובע חוק המחשבים, בהתאם להצעת החוק, פרק נזיקי הנועד להגן על האינטרסים השונים של בעלי המחשב ושל המשתמשים בו, וכן מספר תיקוני חקיקה בתחום דיני הראיות ודיני החיפוש והתפיסה בלבד.

42 הצעת חוק המחשבים, התשנ״ד-1994. ה״ח 2278 התשנ״ד (13.6.1994).

43 בדומה לחוק הבריטי Computer Misuse Act 1990.

יתירה מזו, נראה, כי ההגדרות הקבועות בחוק המחשבים אשר נקבעו לפני עשור שנים הינן מסורבלות ואינן מתאימות לעידן האינטרנט והסלולר של היום. יצוין לעניין זה, כי ההגדרות הקיימות בחוק המחשבים נלקחו מטיוטת תזכיר החוק משנת 1987 (תזכיר שלגי), ולמותר לציין כי דואר זבל רב עבר בים האינטרנט ובמרחב הקיברטי מאז. נראה, כי ההגדרות אינן תואמות כלל את עולמנו העכשווי והעתידי.

קחו, למשל, את ההגדרה של ״שפה קריאת מחשב״ (צורת הבעה המתאימה למסירה, לפירוש או לעיבוד על ידי מחשב או מחשב עזר בלבד) המשמשת רכיב בהגדרת ״מידע״ (נתוני סימנים, מושגים או הוראות, למעט תוכנה, המובעים בשפה קריאת מחשב..). ״מידע״ הינו אחד משני מרכיביו של המונח ״חומר מחשב״ (תוכנה או מידע), אשר מהווה יסוד מרכזי וחשוב בהוראות החוק.

שרשרת ההגדרות שלעיל מעלה את השאלה – האם מידע חייב להיות מובע באופן המתאים למסירה, לפירוש או לעיבוד על ידי מחשב **בלבד**?[44] חדירה לקבצי עיבוד תמלילים, למשל, הינה חדירה למידע אשר ניתן למסירה, לפירוש ולעיבוד על ידי בני אדם, ולכן נראה כי חדירה מעין זו אינה עולה בהגדרה של חדירה אסורה לחומר מחשב.

לא רק זאת, כי אם גם ההפרדה בין הגדרת המונח ״מידע״ להגדרת המונח ״תוכנה״ הינה הפרדה מיותרת. בעידן שבו כל מכשיר סלולרי הינו מחשב לכל דבר ועניין, יש להיעזר בהגדרות שונות ורחבות יותר, או להימנע מהן בכלל.

בסופו של דבר, יש לזכור, כי חוק המחשבים חוקק בתקופה בה הייתה סביבת העבודה מול המחשב שונה מזו המתרחשת היום. די לעיין בפרוטוקולים של ועדת המשנה להצעת חוק המחשבים על מנת להבין עד כמה השתנתה המציאות הטכנולוגית והתפישה המשפטית בעשור האחרון. לפיכך, כל המקדים לתקן את ההגדרות – הרי זה משובח!

תיקונו של חוק המחשבים, על מנת להתאימו לעידן המקוון העכשווי והעתידי, צריך להיות מגובה בעיבוי מערך החקירה והתביעה, תוך גיבושה של פסיקה מספקת, הן בכמותה והן באיכותה.[45]

סוגיה מעניינת נוספת, שקצרה היריעה מלהתייחס אליה במאמר זה, עוסקת בבעיות האכיפה הבינלאומית של עבירות מחשב בכלל, ועבירות חדירה למחשב בפרט, שכן רבים המקרים בהם העבריין נמצא מחוץ לגבולות השיפוט של מדינת ישראל. בשנת 2001 נחתמה אמנה בינלאומית למלחמה בעבירות מחשב ואינטרנט על ידי 26 מדינות האיחוד האירופי וכן על ידי ארה״ב, יפן דרום אפריקה וקנדה. האמנה מחייבת את המדינות החתומות לחוקק חוקים העוסקים בחדירה בלתי מורשית למחשבים, וכן

44 וראו גם ח׳ רביה ״פיל לבן – עשור לחוק המחשבים״ http://law.co.il/showarticles.php?d=h&article=245.

45 **שם**.

לשתף פעולה בנושאי אכיפה.[46] ישראל אינה צד לאמנה, אך אין ספק כי תזקק לשיתוף פעולה בינלאומי על מנת להתגבר על עבירות מחשב במקרים רבים בעתיד או תידרש על ידי מדינות אחרות לסייע בנושא זה.

46 See Council of Europe, Convention on Cybercrime, opened for signature Nov 23, 2001, E.T.S No 185. להרחבה בנושא זה: R. W. Downing "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" 43 **Colum. J. Transat's L.** (2005) 705.